[Gami*et al.*, 5(6): June, 2016]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

EDGE TECHNOLOGIES IN IoT AND APPLICATION SCENARIO OF RFID BASED IoT

Dharam Gami [*], Asst. Prof. Dhaval Nimavat, Asst. Prof. Shubham Sharma
[*] Department of Computer Engineering , Atmiya Institute of Technology and Science, Rajkot, INDIA

ABSTRACT

Internet of Things possesses the power to change the era. IoT will offer an advance connectivity between objects which will change the face of machine-to-machine communication. IoT will connect autonomous systems, devices and heterogeneous machines and make them communicate without human interactions. Many technologies will play significant role in IoT implementation. In this paper, we aim to describe the candidate of edge technologies in IoT and demonstrate how RFID based IoT system will look like with an example of real time application scenario. We show the functional level IoT architecture and essential steps of IoT system.

KEYWORDS: IoT, RFID based IoT, IoT architecture, edge technology, BLE in IoT, IoT Applications.

INTRODUCTION

The term IoT was first coined by Kevin Ashton in 1992. IoT don't have any exact or wildly accepted definition. We can explain IoT by saying that ―IoT is a network of things, where thing refers to a smart object. Objects are embedded with electronics, software, sensors, and network connectivity, which enable these objects to collect and exchange data [5]. Idea behind IoT is to connect things to internet and establish communication between them. IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond automation and machine-to-machine communications (M2M) and covers a variety of technologies, domains, and applications. IoT implementation requires to leverage the existing technologies and infrastructure. Where and when to use which technology and how to accommodate them to fulfil the purposes of IoT are open questions for all. Key challenge areas in IoT are Privacy, Identity Management, Security and Access control, standardization, interoperability and data deluge [3].

True perceptions about IoT:

1. IoT is not a technology: IoT is an idea or a concept whose implementation requires other technologies to participate. These technologies can be anything that fits the need.
2. IoT is not an alternative name of Automation: IoT is more than just automation. However automation is a primary requirement to implement IoT.
3. IoT is not an instance of Artificial Intelligence: IoT do not possess any decision making algorithm unlike AI. In fact, the word 'intelligence' is missing in the concept of IoT. However IoT may help to develop AI systems.

IoT ARCHITECTURE

IoT architecture should possess the characteristics of SOA. Basic requirements of architecture are open loop, scalable, adaptable, flexible and reliable [1]. IoT architecture has not been standardized yet. It will depend on the nature of applications, scope of applications and the type of involved objects as well. However, the functionality of the system can be specified. Essential steps in IoT are (1) Identification (2) Communication (3) Authentication.

(1) Identification: To make communication possible among entities over Internet, it is crucial to ensure the unique identity of the objects. Technologies, that can be used to identify things in IoT, are known as "Edge Technologies" [2]. Technologies like RFID, Bluetooth, BLE and Zigbee can be used as edge technology.

(2) Communication: Once things are given unique identity, they are now capable to communicate using various protocols. This step retrieves the identity of communicating object, passes the identity to respective servers and establishes communication between participating entities. For this purpose, we can use technologies like Wifi, 2G, 3G, GSM, GPRS, etc. Any the technology, which is used to exchange and transport the data (any kind of data), may be used here.

(3) Authentication: Once communications is established, we have to authenticate source, destination, and intermediate entities with respect to each other. It is crucial to ensure that only authenticated entities can participate and only perform authorized actions.

Based on the essential steps, basic three layers IoT architecture can be described as follows [1]:

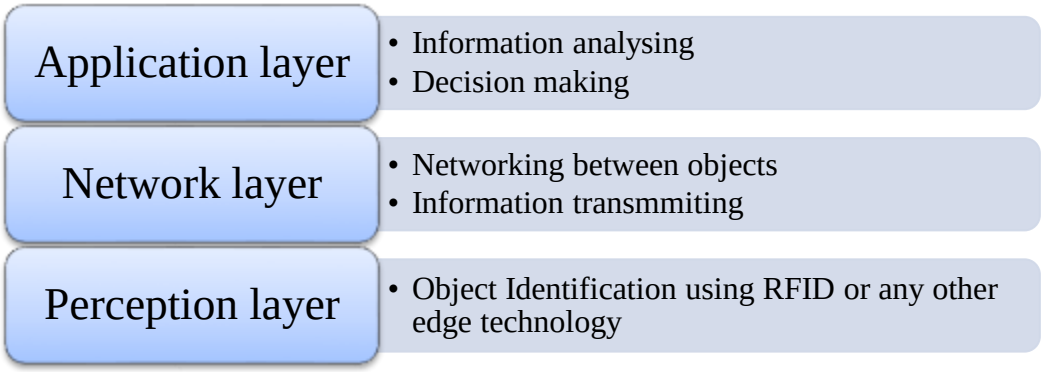


Figure 1: 3-layer IoT Architecture

Edge Technologies:
Among all the candidate of edge technologies, we realized that BLE, Zigbee and RFID are good candidates.

(1) RFID [8]**:**

- RFID has three components: Tag, Reader and server. Tags are of three kinds: Passive, semi-passive and active. Here, we can use semi-passive or active tags. RFID can be used with variety of frequency bands which ranges from 10cm to 200m.
- RFID frequency bands:

Table 1: RFID Frequency Band

Band	Range
120–150 kHz (LF)	10 cm
13.56 MHz (HF)	10 cm –1 m
433 MHz (UHF)	1–100 m
865-868 MHz 902-928 MHz (UHF)	1–12 m
2450-5800 MHz	1–2 m
3.1–10 GHz (microwave)	to 200 m

- Drawback: Power is limited in case of passive and semi passive tags. Passive tag cannot do any computations and semi-passive can do little computation. Size of the active tag is larger than passive tag.

(2) BLE [6] [10]**:**

- **Specifications:**
  - IEEE standard- 802.15.1
  - Range- 10m to 100m

- Data transfer rate- 1Mbps to 24 Mbps

➢ Now a day, sophisticated electronic devices are less with Bluetooth. So, rather to install new technology to make that device smarter, we can use Bluetooth.
➢ Bluetooth can be used for identification and communication. Moreover, it can do mutual authentication.

(3) Zigbee [7]**:**

➢ **Specifications:**
- IEEE Standard- 802.15.4
- Data transfer rate- low (20kb to 250kb)
- Range- 10 to 100 meter
- Security- 128 bit symmetric key
- Connection type- connection oriented

➢ Useful in monitoring and remote control applications
➢ Drawback: Useful in PAN only and cannot handle node mobility. ZigBee is not a frequency hopping technology. So, it requires careful deployment is needed to ensure that there are no interfering signals in the vicinity.

Comparative analysis of edge technologies:

➢ Parameter based comparison [4][9][11]:
- **Power Consumptive (**at object side**)**
  - RFID < BLE<Zigbee < Bluetooth
- **Cost**
  - RFID < BLE <Zigbee< Bluetooth
- **Deployment Complexity**
  - RFID < BLE < Zigbee < Bluetooth
- **Hardware Complexity**
  - RFID < Zigbee < BLE < Bluetooth

.

RFID BASED IoT

How RFID can be used over IoT:

➢ We can put the RFID tag on the object that we want to make smart.
➢ Primary requirement:
➢ Open loop System
➢ It means- "Each RFID tag can be read by Any RFID Reader as well Each RFID reader can read Any RFID Tag"
➢ Tag-Reader link - radio frequency link while
➢ Reader-server link – LAN, WiFi, WLan, Internet.
➢ **Challenges:** Privacy and identity management, power consumption, use of passive tag, computation overhead and issue of reader compromise [12] are major challenges in RFID based IoT.

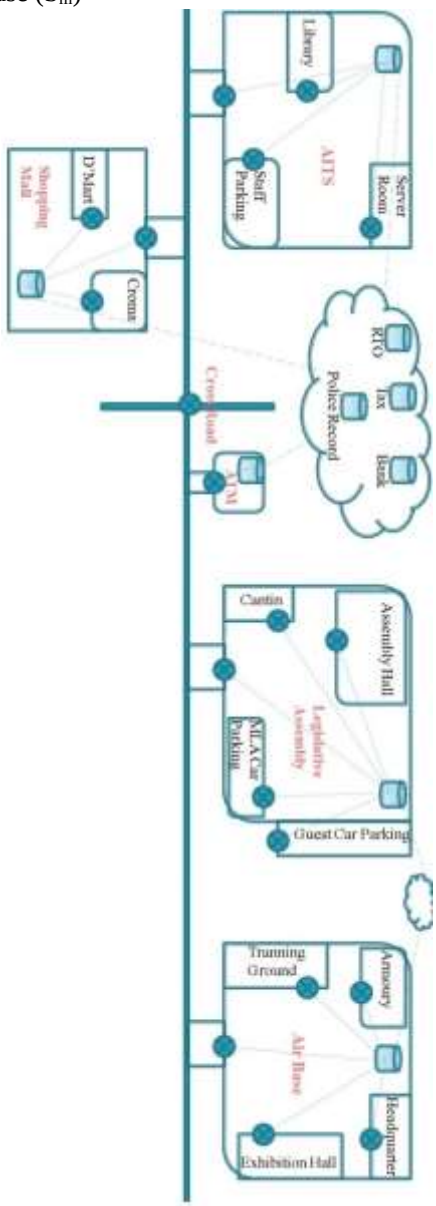
Real Time Application Scenario of RFID based IoT:

➢ To demonstrate the application scenario, We made following assumptions:
- Every person in India has a **unique SmartID** (semi-passive RFID tag)
- Every vehicle in India has a **unique VehicleID**
- Every reader is connected to at least one server
- All the servers form a distributed network and so that, each server can identify all the RFID tags (both SmartID and VehicleID)
- Banking services and all other governmental services which provides the information which comes under RTI will be provided to all the servers over IoT through cloud service. It means the information "if a person has criminal record or not" comes under RTI then each and every server can access this information for each SID.

➢ denotes RFID Reader (R_j)

ISSN: 2277-9655
Impact Factor: 4.116

- Denotes Server/Database (S_m)



. Figure 2: RFID based real time Application Scenario

- ***Explanation:***
  - SID_1 is about to enter AITS with its car VID_1. So, R_1 reads SID and VID and send identity to server of AITS S_1 to get idea that who tries to enter and then authenticate them.
  - SID_1 will try to park car in Staff parking but reader at the gate will authenticate them and allow if and only if SID_1 is a staff member.
  - SID_1 will enter into library where reader at library reads SID_1 and server of AITS authenticate him/her if it is authenticated.
  - After some time, SID_1 will go to shopping mall where the reader at the gate reads SID_1 and authenticate it based on permissions set to server of the shopping mall.
  - SID_1 will use its card to make payment where 'payment reader' will identify the person, then its bank account will be linked and transactions will be carried out.

- After some time SID_1 will pass the cross road with its vehicle VID_1 where reader at the cross road identify them and will use them for governmental purpose or others. Here, stolen vehicles and unregistered vehicles can be tracked easily.
- SID_1 can also be used to withdraw money from ATM.

After some times, the person may visit other area where particular reader, put on that area, will authenticate. This scenario has only two types of objects over IoT, those are human and vehicles.

Applications:

- Keep track of human activity and trace malicious activity.
- Keep track of all vehicles without using GPS.
- Easily trace the stolen, unregistered and illegal vehicles.
- Traffic Control and Management
- Home and industry automation
- Cashless transactions
- Automatic tax deduction

CONCLUSION

IoT needs many technologies to be interoperable to develop it in its true meaning. We have to explore all the existing technologies and invent some new, if required, to find the suitable technology as per need and application. IoT architecture is not standardized but essential functions in IoT are identification, communication and authentication. Among all technologies like RFID, Bluetooth, BLE and ZigBee, RFID be a better candidate for edge technology in IoT implementation because RFID satisfies most of the requirements of IoT and is efficient in terms of power consumption and computational overhead. Enhancement in RFID technology will makes it better to use in IoT. The bottom line in research is to lower the power consumption and reduce the computational overhead.

ACKNOWLEDGEMENTS

It is indeed a great pleasure to express my thanks and gratitude to Prof. Pinaki Ghosh for his valuable suggestions.

REFERENCES

[1] Dharam J. Gami, “IoT: The Age of Machine”, International Journal of Engineering Research and General Science Volume 3, Issue 6, November-December, 2015
[2] Lu Tan, Neng Wang, “Future Internet: The Internet of Things”, 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)
[3] Louis COETZEE, Johan EKSTEEN, “The Internet of Things – Promise for the Future? An Introduction”, IST-Africa 2011 Conference Proceedings
[4] J. Lee, Y. Su, C. Shen, “A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi”, *IEEE IECONN, Nov. 2007, pp. 46 – 51*
[5] https://en.wikipedia.org/wiki/Internet_of_Things
[6] https://en.wikipedia.org/wiki/Bluetooth
[7] https://en.wikipedia.org/wiki/ZigBee
[8] https://en.wikipedia.org/wiki/Radio-frequency_identification
[9] Artem Dementyev, Steve Hodges, Stuart Taylor and Joshua Smith, “Power Consumption Analysis of Bluetooth Low Energy, ZigBee and ANT Sensor Nodes in a Cyclic Sleep Scenario” Microsoft Research, Cambridge, United Kingdom
[10] Carles Gomez, Joaquim Oller and Josep Paradells, “Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology”, Sensors 2012, 12, doi:10.3390/s120911734
[11] http://www.digikey.com/en/articles/techzone/2011/aug/comparing-low-power-wireless-technologies
[12] Imran Erguler, “A potential weakness in RFID-based Internet-of-things systems”, Pervasive and Mobile Computing 20 (2015) 115–126, Elsevier